Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

March 2, 2011

Virginia Information Technologies Agency

ISOAG March 2011 Agenda

I.	Welcome & Opening Remarks	John Green, VITA
II.	Cyber Security in Virginia	Lawrence 'Chip' Muir, Ass't Attorney General of VA / Computer Crimes
III.	Commonwealth Security & Risk Management Panel Discussion	Benny Ambler, Bob Baskette, Michael Watson, VITA
IV.	General Assembly Bills	John Green, VITA
V.	Upcoming Events & Other Business	John Green, VITA
VI.	Partnership Update	Bob Baskette, VITA Michael Clark, NG

Cyber Security in Virginia

Chip Muir
Assistant Attorney General of Virginia
Computer Crime Section

What we will cover

- About the Computer Crime Section
  - A brief overview of the crimes we prosecute
  - Our interest in cyber security from a law enforcement standpoint
- Federal cyber security efforts
- Contemplated cyber security initiatives in Virginia

About the Computer Crime Section

- The Computer Crime Section of the Office of the Attorney General consists of prosecutors and investigators. We offer many different services to the local law enforcement agencies within Virginia.
- The Computer Crime Section primarily involves itself with investigations and prosecutions under the Computer Crimes Act (§ 18.2-152.1 through § 18.2-152.16), as well as child exploitation cases and identity theft cases. We can also assist with the handling of digital evidence in other cases.
- From a prosecution standpoint, our Section does everything from advising during trial preparation to prosecuting the case on behalf of the Commonwealth. From an investigation standpoint, we assist and advise or handle investigations from the time of the complaint.
- We cooperate with sheriff's offices, police departments, and Commonwealth's Attorneys offices throughout Virginia. We invite you to call or email our section with questions on any of the above crimes.

The Computer Crime Section

- The majority of our cases are federal child pornography cases done in conjunction with US Attorney's Offices in Virginia through Project Safe Childhood
- The bulk of our remaining cases involve state child pornography cases
- We have jurisdiction over the Computer Crimes Act, but we are not receiving case referrals in these cases.
- Why?

The Computer Crime Section

- In my view, the role of a prosecutor is to protect the natural rights of our citizens and businesses to life, liberty, and property
- Property protection does not simply mean prosecuting people who steal televisions or candy bars
- It doesn't just mean prosecuting vandals
- It also means protecting wealth property, which often times means protecting the intellectual property of Virginia businesses

The Computer Crime Section

- In 2005, the FBI estimated the annual loss due to cyber crime to be $67 billion.
- Database breach notifications received
  - Since July 2008, the Computer Crime Section has received over 400 database breach notification letters.
  - The estimated cost of a database breach is $8 per record, or $202 per person.
- These losses should be recoverable from the cyber criminals.

The Computer Crime Section

- Good law enforcement starts with great crime prevention
- We want to make sure that criminals do not prey on the citizens and businesses of Virginia
- I would like to see the Computer Crime Section prosecute computer intrusion cases
- If a cyber criminal has caused a financial loss to your business, has stolen your research and development, has taken down your information technology, we should not stand for that.
- There may be valid business concerns to keep an intrusion quiet, but just taking the loss does nothing to discourage thieves. We should fight back.

The Computer Crime Section

- If you think your business could and should prosecute cyber criminals, please contact us.
- The GAO identified reporting cybercrime to the police as the number one recommendation for how to deal with these losses. It's so obvious, but the reports are not forthcoming.
- We can work with you on how to work with investigators and putting a case together.

The Computer Crime Section

- Applicable criminal and civil statutes within the Computer Crimes Act

The Computer Crime Section

- § 18.2-152.4. Computer trespass; penalty.
- A. It shall be unlawful for any person, with malicious intent, to:
- 1. Temporarily or permanently remove, halt, or otherwise disable any computer data, computer programs or computer software from a computer or computer network;
- 2. Cause a computer to malfunction, regardless of how long the malfunction persists;
- 3. Alter, disable, or erase any computer data, computer programs or computer software;
- 4. Effect the creation or alteration of a financial instrument or of an electronic transfer of funds;
- 5. Use a computer or computer network to cause physical injury to the property of another;
- 6. Use a computer or computer network to make or cause to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs or computer software residing in, communicated by, or produced by a computer or computer network;
- 8. Install or cause to be installed, or collect information through, computer software that records all or a majority of the keystrokes made on the computer of another without the computer owner's authorization; or
- 9. Install or cause to be installed on the computer of another, computer software for the purpose of (i) taking control of that computer so that it can cause damage to another computer or (ii) disabling or disrupting the ability of the computer to share or transmit instructions or data to other computers or to any related computer equipment or devices, including but not limited to printers, scanners, or fax machines.
- B. Any person who violates this section is guilty of computer trespass, which shall be a Class 1 misdemeanor. If there is damage to the property of another valued at $1,000 or more caused by such person's act in violation of this section, the offense shall be a Class 6 felony. If a person installs or causes to be installed computer software in violation of this section on more than five computers of another, the offense shall be a Class 6 felony. If a person violates subdivision A 8, the offense shall be a Class 6 felony.

The Computer Crime Section

- § 18.2-152.5. Computer invasion of privacy; penalties.
- A. A person is guilty of the crime of computer invasion of privacy when he uses a computer or computer network and intentionally examines without authority any employment, salary, credit or any other financial or identifying information, as defined in clauses (iii) through (xiii) of subsection C of § 18.2-186.3, relating to any other person. "Examination" under this section requires the offender to review the information relating to any other person after the time at which the offender knows or should know that he is without authority to view the information displayed.
- B. The crime of computer invasion of privacy shall be punishable as a Class 1 misdemeanor.
- C. Any person who violates this section after having been previously convicted of a violation of this section or any substantially similar laws of any other state or of the United States is guilty of a Class 6 felony.
- D. Any person who violates this section and sells or distributes such information to another is guilty of a Class 6 felony.
- E. Any person who violates this section and uses such information in the commission of another crime is guilty of a Class 6 felony.
- F. This section shall not apply to any person collecting information that is reasonably needed to (i) protect the security of a computer, computer service, or computer business, or to facilitate diagnostics or repair in connection with such computer, computer service, or computer business or (ii) determine whether the computer user is licensed or authorized to use specific computer software or a specific computer service.

The Computer Crime Section

- § 18.2-152.12. Civil relief; damages.
- A. Any person whose property or person is injured by reason of a violation of any provision of this article or by any act of computer trespass set forth in subdivisions A 1 through A 8 of § 18.2-152.4 regardless of whether such act is committed with malicious intent may sue therefor and recover for any damages sustained and the costs of suit. Without limiting the generality of the term, "damages" shall include loss of profits.

Proposed Federal Regulation

Proposed Federal Regulation

- Cyber Security has become the primary focus for the House and Senate Homeland Security Committees.
- President Obama has commissioned studies on cyber security that have been broad ranging.
- Numerous bills have addressed cyber security roles and responsibilities at the federal level.
- One bill stands out amongst all the others.

Proposed Federal Regulation

- The "Cybersecurity and Internet Freedom Act of 2011"
- Proposed out of the Senate Homeland Security Committee
- Patroned by Senators Joe Lieberman and Susan Collins
- The bill primarily affects private companies through federal executive empowerment

Proposed Federal Regulation

- Innocuous provisions of the Act
  - Boosting of federal cyber security personnel
  - Improving the federal information technology systems and networks
  - Increased research funding
    - Developing safer new Internet Protocols

Proposed Federal Regulation

- Some aspects of the bill are very controversial
- Events in the Middle East have made these provisions even more controversial
- The bill, in its previous form, picked up the nickname “The Internet Kill Switch”
- Now that Egypt and Libya have shut down their Internet this year during the protests, critics are re-visiting their opinion of this bill

Proposed Federal Regulation

- Executive Powers
  - The President is given the power to declare a "national cyberemergency"
  - If that happens, then the Department of Homeland Security has certain powers to take drastic action
    - Primary power: to tell any private network that they must comply with any federal emergency action, including a total shutdown of the network
  - Cyberemergency can be declared for 30 days, and extended for another 30 day period

Proposed Federal Regulation

- No notice has to be given to the private companies that these actions will be taken
- The power only extends over critical Internet infrastructure
  - However, private networks can be added to the list immediately
  - These companies would also be forced into immediate compliance
- There seems to be no due process allowance to object to the emergency management
- There seems to be no mandatory consultation with the private company

Proposed Federal Regulation

- There is no front end judicial review
- The President does not need to receive authority from a federal judge to make the declaration
- Homeland Security does not need judicial review to impose the emergency action
- Senator Lieberman says judicial review is implicit
  - A private business that sues the federal government will have to successfully claim the emergency action was not the “least disruptive means” feasible

Proposed Federal Regulation

- Critical Infrastructure
  - The Department of Homeland Security assembles the list of assets they deem to be critical infrastructure
  - Assets (which can be publicly or privately owned) are then subject to the President's emergency powers

Proposed Federal Regulation

- Critical Infrastructure Determination Criteria
  - Computer system: servers, routers, web sites, networks, pipelines, SCADA systems, etc.
  - First: the disruption of the system could cause "severe economic consequences" or worse
    - Example could be the power grid, where a cyber attack from a logic bomb would be a serious economic consequence and a public safety catastrophe
  - Second: the system must be a component of the national information infrastructure, or reliant upon the national information infrastructure

Proposed Federal Regulation

- Criteria, continued
- Third, it can't be on the list solely because of First Amendment issues
  - This would be a reaction to concerns from the actions in Libya and Egypt
  - The US cannot put Facebook on the list solely because political protests can be made on the Facebook forum

Proposed Federal Regulation

- "Business-friendly" improvements to the version put forward on February 17 include
  - Private companies may object to placement on the list, and therefore would be exempt from emergency management
    - The suit must be filed in the District of Columbia

Proposed Federal Regulation

- Giving guidelines to the criteria
- Senators hope DHS interprets the severe economic consequence language to mean a $25 billion shock to the economy
  - No criteria on how to measure that (e.g. lost productivity?)
- Other criteria includes mass casualties or evacuations (e.g. Stuxnet causes a SCADA system to malfunction, causing a nuclear explosion) or “severe degradation” to national security

Proposed Federal Regulation

- Adverse reactions from businesses and commentators
- Civil liberties and technology groups have already lined up against the bill, based on the theoretical powers coupled with the practical demonstrations abroad
- ACLU: President still has too much power to interfere with the Internet and recommends requiring DHS to get a court order to implement the emergency actions
- Electronic Frontier Foundation: President has unchecked power to say who and what can and cannot be connected to the Internet during an emergency
- Former Republican Congressman Bob Barr: DHS erroneously shut down 84,000 web sites last year alone
- CATO: Unconstitutional taking of private property under the Fifth Amendment, and doesn't actually improve cyber security on the front end.

Proposed Federal Regulation

- The Fifth Amendment of the Bill of Rights of the United States Constitution
- No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, *nor be deprived of life, liberty, or property, without due process of law*; *nor shall private property be taken for public use, without just compensation.*

Contemplated Virginia Cyber Security Initiatives

Contemplated Virginia Cyber Security Initiatives

- The Commonwealth of Virginia is well positioned to become the most cyber secure state in the country, and to use that position as an economic boon for investment and job creation.
- We want to win on two fronts:
  - Public safety
  - Economic development

Contemplated Virginia Cyber Security Initiatives

- Winning in public safety
  - Teach individual citizens best practices for personal cyber security
  - The Attorney General's Office has a presentation it is seeking to give to citizen groups
  - We plan to order mouse pads that will give tips to the citizens on these best practices
  - Prevent cyber criminals from victimizing our citizens and causing significant financial loss to individuals, and possibly passing losses onto the businesses with whom the victimized individual transacts.
  - Just like in larceny cases, we want to protect our citizens from financial loss. The financial losses due to cyber crime can be even greater than the losses due to a standardized larceny.

Contemplated Virginia Cyber Security Initiatives

- Winning in public safety
  - Similarly promote best practices amongst small businesses
  - Over 52% of small to medium businesses have no IT security guidelines
  - Half of small businesses were infected with some kind of malware last year
    - 31% have no anti-spam software, 23% no anti-spyware, and 15% no firewall
    - 13% are operating without any cyber security software at all
  - These businesses are third party custodians of personal identifying information, and financial losses could come to their customers due to the owner's lack of security measures.
  - The expense of complying with a database breach can be enough to sink a small business
  - Source Panda Security survey

Contemplated Virginia Cyber Security Initiatives

- Work with our large businesses
  - Consult with these businesses at the outset of the initiatives
  - Talk to them about their capabilities
    - How can the government assist them?
    - How can they assist the government?
  - Much more on this to follow

Contemplated Virginia Cyber Security Initiatives

- Create a cyber security emergency response team
  - Develop a team consisting of state and local law enforcement, businesses, other government agencies, and colleges to:
    - Identify incoming cyber emergencies
    - Respond to different cyber emergencies
    - Research and develop cyber security innovations to be used by this team, and shared with other states and localities
  - This can be done through the cooperation of the AG's office, OCP, and Congress.
    - Will require the two state agencies to build the team, which leads to…

Contemplated Virginia Cyber Security Initiatives

- The Attorney General's Office and the Governor's Office of Commonwealth Preparedness
  - As prosecutors of computer crimes and as the group that makes plans for emergencies, the two parties have perfectly-aligned interests in promoting cyber security

Contemplated Virginia Cyber Security Initiatives

- Joint actions that should be considered:
  - Revise the Virginia Infrastructure Protection Plan
    - Put in a cyber security plan for public state and local government networks
      - Virginia had a significant breach of health records, leading to a ransom demand
      - Want to focus on front-line security, and continuity of operations on the back-end of an attack or emergency
    - Work with Virginia businesses to create and then implement cyber security plans
      - Encourage every business to have a plan, and explore ways to make that plan as economically-efficient and cost effective as we can

Contemplated Virginia Cyber Security Initiatives

- More joint actions
  - Work with businesses to identify critical cyber-dependent infrastructure, and address plans drafted in partnership
  - Encourage businesses to share information with the government and vice versa
    - What cyber emergencies are businesses vulnerable to that can affect Virginia citizens? What can happen to the Virginia and federal government that will hurt businesses?

Contemplated Virginia Cyber Security Initiatives

- Cyber Security human capital needs
  - Do we have sufficient personnel being trained in Virginia colleges?
    - If not, can we bring the colleges together with private business and public agencies to work on workforce development programs?
    - Four Virginia universities have NSA certified programs
    - Other schools have expressed interest in creating programs
    - How can we effectively build those programs to support the needs of businesses?
    - How can we use these programs to drive job creation in Virginia?

Contemplated Virginia Cyber Security Initiatives

- Critical Infrastructure needs
  - Do we have the pipelines we need?
  - The bandwidth?
  - What infrastructure investments would make our businesses more profitable, and attract new businesses?
  - What technology can we use to make these investments more cyber secure?

Contemplated Virginia Cyber Security Initiatives

- Identify Virginia stakeholders
  - Federal politicians with a stated interest in cyber security include Congressmen Forbes, Wolf, and Goodlatte
  - Businesses that are willing to lend their subject matter expertise to the government in various capacities

Contemplated Virginia Cyber Security Initiatives

- In conclusion, the private and public sector has the opportunity to come together to move Virginia on a number of fronts.
  - Promoting better cyber security at all levels
  - Deterring cyber crime, and prosecuting cyber criminals
  - Creating effective and efficient cyber security plans
  - Building the workforce development programs to achieve these initiatives
  - Leveraging those programs into a driver for economic growth
  - Using these efforts to attract more investment in Virginia

Conclusion

- If you have any thoughts on the proposals laid out, I would like to hear them.
- I believe good government means supporting the needs of our citizens and businesses now, and preparing for the future.
- It’s a team effort in a game that we must win.

Contact Information

- Lawrence “Chip” Muir
  - lmuir@oag.state.va.us
  - 804-786-2071

Virginia Information Technologies Agency

CSRM Panel Discussion

Benny Ambler, Sr Mgr Security Governance
Bob Baskette, Sr Mgr Security Operations & Architecture
Michael Watson, Sr Mgr IT Risk Management

Virginia Information Technologies Agency

General Assembly Legislation Session 2011

John Green
Chief Information Security Officer

Virginia Information Technologies Agency

HB2189

Information Technologies Agency; assist in determining rules for distribution of electronic records.

Virginia Information Technologies Agency; electronic government services. Provides for the Virginia Information Technologies Agency to assist public bodies of the Commonwealth to determine the rules and standards applicable to the acceptance and distribution of electronic records and electronic signatures.***Patron: Roxann L. Robinson***

Status:

01/12/11 House: Prefiled and ordered printed; offered 01/12/11 11102248D
01/12/11 House: Referred to Committee on Science and Technology
01/26/11 House: Stricken from docket by Science and Technology by voice vote

HB2259

Uniform Computer Information Transactions Act; identity credentials.

Provides for the liability or immunity of both providers and licensees of digital identity credentials in the provisioning, providing, and commercially reasonable reliance upon digital identity credentials. The bill also includes technical amendments. ***Patron: Joe T. May***

Status:

01/12/11 House: Prefiled and ordered printed; offered 01/12/11 11102239D
01/12/11 House: Referred to Committee on Science and Technology
02/08/11 House: Left in Science and Technology

Virginia Information Technologies Agency

HB2271

Computer and digital forensic services; exempt from regulation as private security service business.

Exempts from regulation as a private security service business any individual engaged in (i) computer or digital forensic services or in the acquisition, review, or analysis of digital or computer-based information, whether for purposes of obtaining or furnishing information for evidentiary or other purposes or for providing expert testimony before a court, or (ii) network or system vulnerability testing, including network scans and risk assessment and analysis of computers connected to a network. ***Patron: Mark L. Keam***

Status:

01/12/11 House: Prefiled and ordered printed; offered 01/12/11 11102595D
01/12/11 House: Referred to Committee on Science and Technology
01/26/11 House: Reported from Science and Technology with substitute (21-Y 0-N)
01/26/11 House: Committee substitute printed 11104665D-H1
01/27/11 House: Read first time
01/28/11 House: Read second time
01/28/11 House: Committee substitute agreed to 11104665D-H1
01/28/11 House: Engrossed by House - committee substitute HB2271H1
01/31/11 House: Read third time and passed House BLOCK VOTE (98-Y 0-N)
01/31/11 House: VOTE: BLOCK VOTE PASSAGE (98-Y 0-N)
02/01/11 Senate: Constitutional reading dispensed
02/01/11 Senate: Referred to Committee on General Laws and Technology
02/16/11 Senate: Reported from General Laws and Technology (15-Y 0-N)
02/18/11 Senate: Constitutional reading dispensed (40-Y 0-N)
02/21/11 Senate: Read third time
02/21/11 Senate: Passed Senate (40-Y 0-N)
02/25/11 House: Enrolled
02/25/11 House: Bill text as passed House and Senate (HB2271ER)

HB2315

Breach of medical information; adds private entities are required to provide notice.

Notification of breach of medical information. Adds private entities to the list of those entities that are required to provide notice of a database breach involving medical information. Current law applies to state and local governmental entities only. Any entity, public or private, that is required to provide similar notice pursuant to federal law would be exempt from the state requirement. ***Patron: Kathy J. Byron***

Status:

01/12/11 House: Prefiled and ordered printed; offered 01/12/11 11103065D
01/12/11 House: Referred to Committee on Science and Technology
01/26/11 House: Reported from Science and Technology (17-Y 3-N)
01/27/11 House: Read first time
01/28/11 House: Read second time and engrossed
01/31/11 House: Read third time and passed House (94-Y 4-N)
01/31/11 House: VOTE: PASSAGE (94-Y 4-N)
02/01/11 Senate: Constitutional reading dispensed
02/01/11 Senate: Referred to Committee on Education and Health
02/09/11 Senate: Assigned Education sub: Health Care
02/17/11 Senate: Stricken at request of patron in Education and Health (15-Y 0-N)

HB2317

Information Technology Advisory Council; advise CIO on creation of technology application framework.

Requires the ITAC to advise the Chief Information Officer on the creation of a technology application governance framework through which executive branch agencies can address agency business needs with potential information technology solutions. Agency leaders and information technology managers shall participate with the ITAC in the design of this framework.
Patron: Kathy J. Byron

Status:

01/12/11 House: Prefiled and ordered printed; offered 01/12/11 11103592D
01/12/11 House: Referred to Committee on Science and Technology
02/02/11 House: Reported from Science and Technology (21-Y 0-N)
02/03/11 House: Read first time
02/04/11 House: Read second time and engrossed
02/07/11 House: Read third time and passed House BLOCK VOTE (99-Y 0-N)
02/07/11 House: VOTE: BLOCK VOTE PASSAGE (99-Y 0-N)
02/08/11 Senate: Constitutional reading dispensed
02/08/11 Senate: Referred to Committee on General Laws and Technology
02/16/11 Senate: Reported from General Laws and Technology (12-Y 0-N)
02/18/11 Senate: Constitutional reading dispensed (40-Y 0-N)
02/21/11 Senate: Read third time
02/21/11 Senate: Passed Senate (40-Y 0-N)
02/25/11 House: Enrolled
02/25/11 House: Bill text as passed House and Senate (HB2317ER)

SB943

Information Technology Advisory Council; advise CIO on creation of technology application framework.

Requires the ITAC to advise the Chief Information Officer on the creation of a technology application governance framework through which executive branch agencies can address agency business needs with potential information technology solutions. Agency leaders and information technology managers shall participate with the ITAC in the design of this framework.

Patron: Janet D. Howell

Status:

01/10/11 Senate: Prefiled and ordered printed; offered 01/12/11 11103591D
01/10/11 Senate: Referred to Committee on General Laws and Technology
01/19/11 Senate: Reported from General Laws and Technology (15-Y 0-N)
01/21/11 Senate: Constitutional reading dispensed (35-Y 0-N)
01/24/11 Senate: Read second time and engrossed
01/25/11 Senate: Read third time and passed Senate (39-Y 0-N)
02/07/11 House: Placed on Calendar
02/07/11 House: Read first time
02/07/11 House: Referred to Committee on Science and Technology
02/16/11 House: Reported from Science and Technology (21-Y 0-N)
02/17/11 House: Read second time
02/18/11 House: Read third time
02/18/11 House: Passed by temporarily
02/18/11 House: VOTE: BLOCK VOTE PASSAGE (95-Y 0-N)
02/24/11 Senate: Enrolled
02/24/11 Senate: Bill text as passed Senate and House (SB943ER)
02/24/11 House: Signed by Speaker
02/24/11 Senate: Signed by President

HJ577

Internet; urging Congress to recognize importance of unfettered access and limit regulation by FCC.

Memorializes Congress to recognize the importance of unfettered access to the Internet. Urges Congress to limit the Federal Communications Commission's authority over regulation of the Internet.
Patron: John M. O'Bannon, III

Status:

01/10/11 House: Prefiled and ordered printed; offered 01/12/11 11103326D
01/10/11 House: Referred to Committee on Rules
01/25/11 House: Reported from Rules (15-Y 0-N)
01/28/11 House: Passed by for the day
01/31/11 House: Taken up
01/31/11 House: Pending question ordered
01/31/11 House: Engrossed by House
01/31/11 House: Agreed to by House (63-Y 33-N 3-A)
01/31/11 House: VOTE: ADOPTION (63-Y 33-N 3-A)
02/01/11 Senate: Reading waived
02/01/11 Senate: Referred to Committee on Rules
02/21/11 Senate: Left in Rules

HJ645

Local governments; procurement and sharing of technology applications, report.

Study; procurement and sharing of technology applications for local governments; report. Requests the Secretary of Technology to study opportunities to facilitate cooperative procurement and sharing of custom technology applications to leverage buying power and create efficiencies for local government. ***Patron: Charles D. Poindexter***

Status:

01/12/11 House: Prefiled and ordered printed; offered 01/12/11 11103712D
01/12/11 House: Referred to Committee on Rules
01/18/11 House: Assigned Rules sub: #3 Studies
01/27/11 House: Subcommittee recommends reporting with amendment(s) (4-Y 0-N)
02/01/11 House: Reported from Rules with amendment (15-Y 0-N)
02/04/11 House: Taken up
02/04/11 House: Committee amendment agreed to
02/04/11 House: Engrossed by House as amended HJ645E
02/04/11 House: Printed as engrossed 11103712D-E
02/04/11 House: VOTE: BLOCK VOTE ADOPTION (96-Y 0-N)
02/07/11 Senate: Reading waived
02/07/11 Senate: Referred to Committee on Rules
02/14/11 Senate: Assigned Rules sub: #1
02/18/11 Senate: Reported from Rules by voice vote
02/21/11 Senate: Reading waived (39-Y 0-N)
02/22/11 Senate: Read third time
02/22/11 Senate: Agreed to by Senate by voice vote

Upcoming Events

Gartner Group Webinar Series

Free Web seminars offered by the Gartner Group

These one-hour sessions feature tactical advice with an emphasis on reducing costs. Examples of webinars offered:

***Portals: Emerging Demands and Technologies Will Change the Market**

***Top 10 Trends Shaping Infrastructure & Operations**

***Technology Trends You Can't Afford to Ignore**

***The Big Migration: Windows 7 and Office 2010**

Visit the link to Gartner* below to see the full listing of the topics offered and take advantage of these educational opportunities.

* **http://my.gartner.com/portal/server.pt?open=512&objID=202&mode=2&PageID=3428358&webinarAction =webinarsGotoPage&we binarType=upcoming&page=2**

ISSA Spring Study Group

2011 CISSP Spring Study Group

The Central VA Chapter of ISSA is in the process of forming the Spring `11 CISSP Study Group.

* **Launch date will be early March with conclusion by end of May.**
* **Participant fee is $450 w/ ISSA membership required.**
* **Space is limited!**

Inquire with Robert Thomas at: *Secretary@issa-centralva.org*

Registration information will be posted online soon.

http://www.issa-centralva.org/Training.aspx

CIO Council

When: Wednesday, March 9th

9a – 12p

Location: CESC

Information Security System Association

ISSA

DATE: Wednesday, March 9, 2011
LOCATION: Maggiano's Little Italy
11800 West Broad Street, #2204, Richmond, VA 23233
TIME: 11:30 - 1:00pm. Presentation starts at 11:45.
Lunch served at 12.
COST: ISSA Members: $20 & Non-Members: $25

SPEAKER: Donald E. Alison, Digital Forensic Examiner
in Stroz Friedberg's Washington, DC, office

TOPIC: "Dipping a Forensic Toe in the Information Ecosystem"

Project Mgmt Professional (PMP) Workshop

When: March 12, 19, 26

Time: Saturday, 8:30a – 5:00p

Where: Hilton Garden Inn, Innsbrook
4050 Cox Rd, Glen Allen, VA

Fee: Members- $595; Non-members- $775

There is a $50 cancellation fee. Seating is limited!

Register at: www.pmicvc.org

Registration closes 3/3/11

AITR Meeting

Wednesday, April 13th

8:30 am – 9:00 am: Networking

9:00 am: Meeting start

Location: *CESC*

National Webcast Initiative

Thursday, April 21
2:00 pm – 3:00 pm EDT

Topic: ***Data Life Cycle Management***

Visit MS-ISAC web for more information:
http://www.msisac.org/webcast/

Virginia Information Technologies Agency

Internet Security Training Workshop

Virginia Tech & SANS Institute are pleased to offer this 6-day SANS program

http://www.cpe.vt.edu/isect/

May 17 – 22, 2011

Torgersen Hall at Virginia Tech
Blacksburg, VA

Who Should Attend:

- ***Penetration testers***
- ***Ethical hackers***
- ***Auditors who need to build deeper technical skills***
- ***Security personnel whose job involves assessing target networks & systems to find security vulnerabilities***

- **Special pricing is available for any faculty/staff from any accredited EDU site (K-12, community college or higher education institution) or member of law enforcement. Commercial or Government employees are also welcome to attend.**

** **If you wish to receive additional information about this program, please contact Randy Marchany, IT Security Lab, Virginia Tech by e-mail at marchany@vt.edu**

Future ISOAG's

From 1:00 – 4:00 pm at CESC

ISOAG will be held the 1st Wednesday of each month in 2011

Wednesday - April 6, 2011

Wednesday - May 4, 2011

Future IS Orientation Sessions

Tuesday - (CESC)	**March 8, 2011**	**1:00 – 3:30p**
Tuesday - (CESC)	**May 10, 2011**	**9:00 – 11:30a**

IS Orientation is now available via webinar!

ISOAG-Partnership Update

IT Infrastructure Partnership Team
Bob Baskette

March 2, 2011

IT INFRASTRUCTURE PARTNERSHIP

VITA

NORTHROP GRUMMAN

ADJOURN

THANK YOU FOR ATTENDING